DoD TELECOMMUNICATIONS and DEFENSE SWITCHED NETWORK CHECKLIST V2R3.2

19 MAY 2006

Developed by DISA for the DOD

Database Reference Number: _____

Database entered by: _____ Date: _____

Technical Q/A by: _____Date: _____

Final Q/A by: _____ Date: _____

CAT I: _____

CAT II: _____

CAT III: _____

CAT IV: _____

Total: _____

UNCLASSIFIED UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Site Name	
Address	
Phone	

Position	**Name**	**Phone Number**	**Email**	**Area of Responsibility**
IAM				
IAO				

PROCEDURES FOR REGISTRATION OF VOICE/VIDEO/RTS ASSETS IN THE VMS

1.1 Introduction

This document will describe the proper procedure to follow to register and update the IA status of voice and/or video / real time services (RTS) systems and devices in VMSv6. For the purpose of this document, we will use RTS to refer to any voice/video/RTS system or device. This includes all types of telecom switches or video systems, whether they are TDM or IP based, as well as any supporting system or device.

1.1.1 Pre - Requisites

Any person that needs to interface with the VMSv6 must:

1. Take the on-line CBT, which can be accessed at https://vmscbt.disa.mil (no login is required). It is highly recommended that a person taking the CBT review all modules to become familiar with all of the roles that the various VMS users fulfill.

2. Download and become familiar with the appropriate users guide for user role(s) that the trainee will be fulfilling. These bay be found at https://vmscbt.disa.mil/resources.htm
3. Obtain a VMS account and login to the application. Instructions for this are contained in the CBT.
4. Become familiar with the navigation and features of VMS by reviewing the CBT and users guide while in VMS.

Once these steps have been completed, one can begin to register assets and update their statuses.

1.2 RTS Asset Naming Convention

A naming convention for the system and its components must be used when registering the various assets so that the individual assets can be more easily identified as a group or part of a system. This naming convention should be based on the name of the owner/site/location/enclave and the name/type of RTS system being registered.

Some examples of an overall RTS system name might be:

- DISA-SKY7_Cisco-VoIP
- Ft.Hood_MSL100
- LacklandAFB_MSL100
- Gunter_CS2100
- Landstuhl_HiPath4000
- SHAPE_EWSD
- Pearl_5ESS

This name represents the Non-Computing Asset for the overall RTS system.

The Computing Assets, that make up the RTS system must include the name of the overall system and a unique name for the device. This unique name should include the function of the device and its network addressable name. That is the unique name that is used to identify the box on the network. This is not the IP address or MAC address, which is entered as an attribute of the asset.

Some examples of component device/system names might be:

- DISA-SKY7_Cisco-VoIP_CCM-Registrar_CCM0001RP
- DISA-SKY7_Cisco-VoIP_CCM-Publisher_CCM0002PP
- DISA-SKY7_Cisco-VoIP_CCM-B/URegistrar_CCM0003RB
- DISA-SKY7_Cisco-VoIP_CCM-B/UPublisher_CCM0004PB
- DISA-SKY7_Cisco-VoIP_PSTN-Gateway_PSTNGW0001
- DISA-SKY7_Cisco-VoIP_DSN-Gateway_DSNGW0001
- DISA-SKY7_Cisco-VoIP_LAN-Core_SKY70001
- DISA-SKY7_Cisco-VoIP_ManagementWS_SKY7MWS0001
- DISA-SKY7_Cisco-VoIP_ManagementLS_SKY7MLS0001

In the event that an asset already exists and uses a different naming convention, place the name derived here the asset ‘Description’ field.

1.3 RTS Asset Identification

An RTS system as a whole is an asset, however, each individual device that makes up the system is also an asset. Each of these assets must be registered in the VMS. VMS has 2 primary types of assets, Computing and Non-Computing.

Each RTS system at a given site/location/enclave needs to be registered as a Non-Computing Asset in the VMS.

The individual assets are registered as Computing Assets. Computing Assets are based on boxes, which have an operating system (OS) as well as applications such as databases, web servers, and control and/or management applications. The OS and the applications are called “Postures” in the VMS. All applicable postures are assigned to the asset.

Typically, a Computing Asset will have at least one IP address and/or one MAC address. Management workstations, LAN switches and routers, firewalls, multiplexers, phones, and similar devices are also Computing Assets that make up the RTS system. Desktops and Laptops are also computing devices that need to be registered.

1.3.1 Local Management System(s)

LAN switches and routers, management workstations/consoles, NMS servers, and front end processors that are used exclusively in the local management the RTS system must be named and registered as part of the RTS system and given a unique name (using the naming convention above) identifying it as part of the RTS system. Local management systems must be treated as an enclave.

1.3.2 Remote Management System(s)

LAN switches and routers, management workstations, NMS servers, and front end processors, etc that are part of a remote management/monitoring system such as ADIMSS, ARDIMSS, ESRS, etc, must be registered by the owner/SA of the device or the owner/SA of the management/monitoring system that it is part of. It is critical that the ‘Location’, ‘Managed By’, and ‘Owned by’ fields are properly filled out. The device or system must also be associated with the proper program(s), site, and enclave under the ‘Sites/Enclaves’ tab. Remote management systems are typically separate enclaves from the local management system enclaves.

1.3.3 BCPS LAN/CAN/BAN Infrastructure

LAN switches and routers that make up the data and RTS distribution system must be named and registered by the LAN/enclave SA in accordance with the Network Infrastructure asset registration instructions found in the Network Infrastructure Checklist. RTS requirements for the LAN are applied to the asset via the Non-Computing asset assignment of the RTS requirements to it as described below.

1.3.4 RTS Adjunct/Auxiliary Systems/Devices

Adjunct/Auxiliary Systems/Devices are defined as systems and devices that augment the basic telephony service. Examples of such systems and devices are: Voice mail systems, call center and/or operator systems, CTI systems, IVR systems, auto-attendant systems, Emergency Services (911) systems, etc. Systems such as these may be registered as part of the RTS system if appropriate (i.e., small systems or single devices), or may be registered as a separate Non-Computing system / enclave asset along with its Computing assets.

1.4 RTS Asset Creation In The VMS

The RTS system Non-Computing Asset(s) is(are) registered first, followed by the Computing Assets. This section will provide an overview of the major steps. Subsequent sections will provide step-by-step procedures.

1.4.1 The Organization, Site, and/or Location

Before assets can be created, an organization and a site or location must be defined in the VMS. This is a VMS ISSM role and responsibility and is outside the scope of this document. Programs are also defined in the VMS and this is the responsibility of the VMS DAA role.

1.5 Non-Computing Asset Creation

First create the Non-Computing Asset for the RTS system using the naming convention described in "RTS Asset Naming Convention" above. On the 'Asset Posture' tab, expand the 'Voice/Video/RTS Policy' item and check the policies that apply. The available policies are:

- DRSN Policy
- DSN Policy
- VoIP/VoSIP Policy

'DRSN Policy' applies to an asset that is part of, or connected to, the DRSN. This can also apply to other "secure" or classified voice/video/RTS systems.
'DSN Policy' applies to an asset that is part of, or connected to, the DSN. or other UN-classified voice/video/RTS systems.. All UN-classified voice/video/RTS systems owned or operated by, or for, the DoD are subject to the same requirements.
'VoIP/VoSIP Policy' applies to an asset being registered that provides IP based voice or video communications (i.e., VoIP). This includes IP centric systems as well as IP enabled TDM based systems.

Either DSN Policy **OR** DRSN Policy must be checked. VoIP/VoSIP Policy must **ALSO** be checked if the system provides IP based voice or video communications.

A local RTS system management LAN, that is not part of the site LAN, should be added to, or registered as part of, the RTS Non-Computing Asset. Additionally, a LAN that only supports an adjunct/auxiliary system to the RTS system, such as a call center or IVR system may be added to or registered as part of the RTS Non-Computing Asset.

This is done by adding the 'Network Infrastructure Policy' and/or the 'General Business LAN Enclave' postures.

Additionally, an adjunct/auxiliary system to the RTS system (and its supporting LAN) such as a call center or IVR system etc, that is not part of the site LAN, may be registered a separate complete system to include its supporting LAN. Such a system is registered as a Non-Computing Asset using the naming convention for the overall RTS system and adding the adjunct/auxiliary system name. For Example:

- LacklandAFB_MSL100_CallCtr-Sys
- LacklandAFB_MSL100_IVR-Sys
- LacklandAFB_MSL100_911-Sys

This is done by adding the 'Network Infrastructure Policy' and/or the 'General Business LAN Enclave' as well as the 'Voice/Video/RTS Policy' postures to the Non-Computing Asset.

The second Non-Computing Asset that needs registration consideration is the site LAN/CAN/BAN that provides distribution for both RTS services and data traffic. This network must be registered along with its components whether it supports RTS systems or not. The SA for the RTS system must work with the SA for the LAN/CAN/BAN to insure that the Voice/Video/RTS Policy asset postures are selected as described above for the RTS System itself. These two SAs could be the same person, however, if not, the SA for the LAN/CAN/BAN should grant "update" permissions on LAN assets to the SA for the RTS system. Asset naming would follow that chosen by the SA for the LAN/CAN/BAN.

Alternately, the SA for the RTS system could create his/her own LAN/CAN/BAN Non-Computing Asset and assign the 'Voice/Video/RTS Policy' asset postures to it. Asset naming would follow the naming convention described in "RTS Asset Naming Convention" above. In this case, the individual LAN/CAN/BAN Computing Assets would not be registered since the SA for the LAN/CAN/BAN would register these.

Detailed step-by-step process instructions are provided under "Creating the Non-Computing Asset(s)" below.

1.5.1 Computing Asset Creation

All system devices must be defined and registered once the appropriate NON-Computing Assets are created, and the BCPS LAN/CAN/BAN has had the Voice/Video/RTS Policies added to it. The SA for the BCPS LAN/CAN/BAN must register each LAN switch, router, and management system. This does not have to be done by the RTS system SA unless he/she is also the SA for the BCPS LAN/CAN/BAN, or if the RTS system SA has created a separate Non-Computing Asset for the RTS BCPS LAN/CAN/BAN.

The following are examples of RTS Computing Assets: (Note: Some of these may have sub-components that are also considered as individual Computing Assets.)

- TDM Switch (Possible sub-components)
- Local Call Controller (Possible sub-components)
- Call Manager Subscriber
- Call Manager Publisher
- Media gateway
- RTS firewall or Boundary control device

- LAN Switch / Router
- Phone instrument – endpoint
- Management workstation
- NMS data collection device or server
- Server (of almost any type)
- VTC MCU (Possible sub-components)
- VTC endpoint
- Gatekeeper
- All GSCR device type designations:
- Many others

All computing assets are registered with an OS. They may also have applications such as databases and/or web servers that also must be added to the posture of the asset.

Registering computing assets is an iterative process until all assets are registered.

Detailed step-by-step process instructions are provided under “Creating the Computing Asset(s)” below.

1.6 Creating Assets – Step-by-Step

1.6.1 Creating the NON-Computing Asset(s)

These instructions apply to creating the RTS system and/or Adjunct/Auxiliary system NON-Computing Asset.

Note: *(Reviewer)* It is recommended that a reviewer work with the Voice/Video/RTS system SA when creating assets for this type of system. The SA will have more knowledge of the system and can assist in making sure that all applicable postures are applied and that the system naming, identification, enclaves, and programs are selected or applied properly.

a. Steps

i. Expand 'Asset Findings Maint'

ii. Click 'Assets/Findings'

iii. **Expand 'By Location'** and then find and expand your site/location. (Others may need to expand 'Managed By' or 'Owned By'. What is seen depends upon your permissions or role.) Within the location, assets are divided into computing, non-computing and CNDS.
- Proceed to step vi.

(Reviewer Only) Expand 'Visits' to display its sub-folders.

iv. *(Reviewer Only)* Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.

v. *(Reviewer Only)* Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.

vi. **Click the 'yellow folder'** icon located at the right of 'Non-Computing'. You may expand 'Non-Computing' to see assets that have already been created and that you have permissions for.

vii. Click the 'General' tab
- Enter a 'Host Name' using the naming convention described in "RTS Asset Naming Convention" above.
- Enter a 'Description' of the system.
  Note: This should reflect a general description of the RTS System and could include the make and version of the LCC software.
- Verify/Select the location of the system in "Location"
- Verify/Select the owner of the system in "Owner": (Used to register asset to parent or child location.)
- Verify/Select the organization or site responsible for management of the system in "Managed By": (Used for remotely managed locations.)
- Verify 'Mac level', 'Confidentiality', & 'Classification', Change as required.
  Note: These default to MAC II, Sensitive, Unclassified. The 'Confidentiality' of a RTS system or asset should never be set to 'Public' since its configuration is considered sensitive. These settings should match those identified in the site or system SSAA.
- Click 'Save'.

Note: It is recommended that you click 'Save' after filling out each tab or more often. This practice will prevent the loss of recently entered data in the event of a timeout. You may wait to save until after filling out all tabs but you must click save at the end of data entry on all tabs or your work will be lost.

viii. **Click the 'Asset Posture' tab** to add functions to the asset:
- Expand 'Non-Computing'
- Expand 'Voice/Video/RTS Policy' (or 'Telecom Policy')
- Check the boxes for appropriate policy/policies as follows:
  - Check 'DRSN Policy' if the asset is part of, or is connected to, the DRSN. **Note**: This policy can also apply to other "secure" or classified voice/video/RTS systems.

  OR
  - Check 'DSN Policy' if the asset is part of, or is connected to, the DSN. **Note**: This apples to ALL UN-classified voice/video/RTS systems whether part of the DSN or not. All UN-classified voice/video/RTS systems owned or operated by, or for, the DoD are subject to the same requirements.

  AND
  - Check 'VoIP/VoSIP Policy' if the system being registered provides IP based communications. This includes IP centric systems and IP enabled TDM based systems.

  AND
  - (Conditional) If there is a LAN that only supports the management of the RTS system or an adjunct/auxiliary system to the RTS system AND it is not part of the site LAN/CAN/BAN or the site's OOB management LAN:
    - Expand 'Network Policy Requirements'
    - Check 'Network Infrastructure Policy'

    Note: If such a LAN is not added here it must be registered separately under both Non-Computing and Computing. Adjunct/auxiliary systems LANs and devices may also be registered separately.

  AND
  - (Conditional) If this LAN has a boundary that touches another LAN, or a local / extended enclave, or a DoD WAN:
    - Expand 'Enclave'
    - Check 'General Business LAN Enclave'.
- Click '>>' to move it to the 'Selected' window (This can be done after each selection or after all selections).
- Click 'Save'

ix. **Click the 'Systems / Enclaves' tab** to associate this asset with the appropriate or all applicable program(s), enclave(s), and site(s).
- Determine the enclave and/or program that the asset is part of.
- In the 'Available Systems' box:
  - Find and select 'DISN-DSN' if the system can place or receive DSN calls.

  OR
  - Find and select 'DISN-DRSN' if the system can place or receive DRSN calls. (Not available as of 4/7/05 See note below)
  - Click '>>' to move it to the 'Selected Systems' window

- Click 'Save' (optional)

AND

- Find and select 'ADIMSS', IF the RTS System is managed or monitored by the ADIMSS (DSN),

OR

- IF the RTS System is managed or monitored by the ARDIMSS or ESRS (DRSN), Find and select 'ARDIMSS' and/or 'ESRS'
- Click '>>' to move it to the 'Selected Systems' window
- Click 'Save' (optional)

o In the 'Available Enclaves' box:

- Find and select the local enclave that the RTS system is part of. (i.e., your site/location)
- Click '>>' to move it to the 'Selected Enclaves' window
- Click 'Save'

Note: For registered enclaves and/or programs, choose all that apply. If the enclave or program is not present, ensure that the IAM [or *(Reviewer Only)* Team Lead] works with the appropriate site personnel to request the enclave or program be added.

x. **Click the 'Additional Details' tab** to add building and room number information for the RTS asset; this should reflect the location of the RTS core equipment.
xi. **Click 'Save'**.
xii. Return to step vi to create another Non-Computing asset or proceed to creating the Computing Assets in the next section.

Note: The above 'Voice/Video/RTS Policy' postures and program association may be added to an enclave or network non-computing asset instead of creating a separate Voice/Video/RTS non-computing asset.

1.6.2 Creating the Computing Assets

These instructions apply to creating the RTS system and/or Adjunct/Auxiliary system Computing Asset(s).

Note: *(Reviewer)* It is recommended that a reviewer work with the Voice/Video/RTS system SA when creating assets for this type of system. The SA will have more knowledge of the system and can assist in making sure that all applicable postures are applied and that the system naming, identification, enclaves, and programs are selected or applied properly.

b. Steps

i. **Expand 'Asset Findings Maint'**
ii. **Click 'Assets/Findings'**
iii. **Expand 'By Location'** and then find and expand your site/location. (Others may need to expand 'Managed By' or 'Owned By'. What is seen depends upon your permissions or role.) Within the location, assets are divided into computing, non-computing and CNDS. Proceed to step vi.
(Reviewer Only) Expand 'Visits' to display its sub-folders.
iv. *(Reviewer Only)* Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.

v. *(Reviewer Only)* Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.

vi. **Click the 'yellow folder'** icon located at the right of 'Computing'.
You may expand 'Computing' to see assets that have already been created and that you have permissions for.

vii. **Click the 'General' tab**
- Enter the 'Host Name' following the naming convention described above.
- Enter a 'Description' of the asset. This should reflect the function and platform of the device. i.e., make and model of the device and software version etc.
- Verify/Select the location of the system in "Location"
- Verify/Select the owner of the system in "Owner": Used to register asset to parent or child location.
- Verify/Select the organization or site responsible for management of the system in "Managed By": Used for remotely managed/monitored locations.
- Verify 'Mac level', 'Confidentiality', & 'Classification', 'Status', 'Use', & 'Workstation', Change as required.
  Note: These default to MAC II, Sensitive, Unclassified, Online, Production, No. The 'Confidentiality' of a RTS system or asset should never be set to 'Public' since its configuration is considered sensitive. These settings should match those identified in the site or system SSAA.
- **Click 'Save'**.
  Note: It is recommended that you click 'Save' after filling out each tab or even more often. This practice will prevent the loss of recently entered data in the event of a timeout. You may wait to save until after filling out all tabs but you must click save at the end of data entry on all tabs or your work will be lost.

viii. **Click the 'Asset Identification' tab** to enter as much identifying information as is available:
- Enter one or all of the following: 'I.P. Address(s)', 'MAC Address(s)', 'System Unique ID'
  Note: The 'System Unique ID' field may be used in addition to the IP and/or MAC addresses. The name used in the 'Host Name' field MAY be entered in the 'System Unique ID' field.
  Note: When entering IP and/or MAC addresses, complete all fields and click 'add'. The address is listed on the right. Multiple addresses can be entered one by one. Addresses can be deleted by clicking 'remove' next to the address to be deleted.
  Note: IPv6 addresses can be entered along with IPv4 addresses. Click 'IPv6' to obtain an IPv6 address box. Click 'IPv4' to revert back to an IPv4 address box. Enter as noted above.

Note: Establish your standards by using the loopback IP address of a network device. If a loopback is not used or is unavailable, use the management interface IP address or MAC address. These entries are not required if the device is not network enabled (i.e., a legacy TDM device that only has a serial management (craft) interface). In this case the device name used in the 'Host Name' field MUST be entered in the 'System Unique ID' field.

- Enter the 'Fully-Qualified Domain Name' of the device if it is a member of a network domain.
- **Click 'Save'**.

ix. **Click the 'Asset Posture' tab** to add Postures or functions to the asset:

a) **Expand 'Computing'** to view the available postures

Note: Expand each of the categories listed throughout the tree and click all applicable boxes for the specific asset being registered. Every asset has an OS. Expand 'Operating System' (and sub-branches) and select the version of OS that is used by the asset. Assets may also have applications. Expand 'Applications' (and sub-branches) and select ALL the application types and versions that are used by the asset. Follow this method for adding all applicable postures or functions to the asset being registered. The following steps will define a more detailed procedure or guide tailored to RTS systems. However, it is impossible to anticipate every possibility with these instructions due to the fact that RTS systems utilize various combinations of all technologies listed. The SA (or reviewer) is responsible for knowing what the asset being registered is, what its OS is, and what other applications or technologies it uses.

Note: Technology based rules within the VMS require the selection of additional postures and/or the input of additional information, such as instance identifiers, when selecting some items in the 'Available Postures' list. Refer to the VMS registration instructions found in the Checklist for the related technology. This is most often related to the Database and Web Server postures. A listing of these rules may be found on the VMS Help page. When this information is required, additional information or input boxes are displayed (following a 'Save) in the lower right corner of the 'Available Postures' under the 'Selected' box. Input boxes are accompanied with a 'add' link that must be clicked to enter the information.

Note: Clicking '>>' can be done after each selection or after all selections. You will need to expand the device name that appears in the 'Selected' box to see the various items selected.

Note: **Rules must be satisfied or the Asset** Posture selection(s) **will not save.** Clicking '>>' will cause any required additional input box to appear under the 'selected' box. This does NOT display alerts. Clicking 'Save' will cause an alert for any rule that is not satisfied to be displayed under the 'selected' box. Additionally, All rules and input boxes that are displayed must be satisfied before the posture will save successfully. Therefore it is recommended that '>>' and 'Save' be clicked after selecting any posture tree under the top level. The instructions will reflect this.

b) **Expand 'Voice/Video/RTS'** to view the available postures or functions. Check all boxes that apply as follows:
Note: If registering a LAN/CAN/BAN network infrastructure device or management system, Expand 'Network' then 'Data Network' and refer to the VMS registration instructions found in the Network Infrastructure, IP Wan, and/or Backbone Transport Checklists.
  - Check 'VoIP Switch/System/Device' if the asset provides, or is involved in providing IP based RTS communications. This includes Voice as well as VTC that is part of or associated with the Voice system. (i.e., video phones or VTC devices or applications that are controlled by or register with a RTS/VoIP LCC. This also includes IP enabled TDM switches.

AND/OR

  - Check 'TDM Switch/System/Device' if the asset is a TDM based telecommunications switch. This includes IP enabled TDM that provide VoIP service. In this case 'VoIP Switch/System/Device' is also checked.
    Note: This also applies to TDM signaling a Switch/System/Device such as an SS7 STP, SSP, or SCP. (Refer to the DSN STIG for an explanation of these devices.)

OR

  - Check 'Voice/Video Adjunct/Aux/Management System/Device' if the asset is involved in managing a RTS system or device or providing some adjunct or auxiliary function to the RTS system other than providing the RTS switching capability.

OR

  - Check 'Video/VTC System/Device' if the asset is, or is part of, a video or VTC system that is NOT controlled by the RTS/VoIP LCC.

- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **'Save'** again.

c) **Expand 'Role'** to view the available Roles for the asset or system being registered. Rules within the VMS require the selection of a Role.
- Check the box next to each role that the asset fulfills. RTS system devices must have one or more of the following selected:

IF the asset is part of a classified RTS system or network

- Check the box next to 'Classified RTS'. This applies to all RTS system assets including core equipment, management systems/devices and Adjunct/Auxiliary systems/devices.

OR IF the asset is used in an UN-classified RTS system

- Check the box next to 'UN-Classified RTS'. This applies to all RTS system assets including core equipment, management systems/devices and Adjunct/Auxiliary systems/devices

AND IF the asset is part of a RTS management system

- Check the box next to 'RTS Management'. This applies to assets that are part of a system that manages core equipment and/or Adjunct/Auxiliary systems/devices.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.

Note: Additional roles may need to be selected due to rules associated with other postures. One of these is the Windows OS, which requires the selection of 'Domain Controller', 'Member Server', or 'Workstation'. These may be selected now if selecting a Windows OS in the next step.

d) **Expand 'Operating System'** to view the available OSs. Drill down through the tree to locate the version of OS installed on the asset. Rules within the VMS require the selection of an OS.

- Check the box next to the OS installed on the asset. Some OSs can be found at the top level of the tree. Others and their versions require drilling deeper. The following steps provide a more in depth procedure and explanation.

IF the asset is based on a Windows OS

- Expand 'Windows' AND expand the Windows version being used.
  - Check the box next to the version of Windows installed on the asset.
    Note: For Windows registration instructions and further explanation, refer to the VMS registration instructions found in the Windows Checklist.
    Note: Rules within the VMS require the selection additional postures when selecting the Windows Operating System. This is covered in the next step.
    Note: If the version of windows being used is a vendor-customized version, check the box next to the version of Windows on which the vendor based their customization.
  - Expand 'Role' and select 'Domain Controller', 'Member Server', or 'Workstation'. RTS core equipment will typically be registered as a 'Member Server' unless it provides Active Directory Services.

Note: Rules within the VMS also add the postures of Application/Browsers/Internet Explorer/IE6 and Application/Desktop Application - General. These appear after the Role rule is satisfied and the selections/Asset is saved. The browser selection may be changed if necessary. See Browser selection below.

OR IF the asset is based on a UNIX or Linux OS

- Expand 'UNIX' AND sub-branches to locate the OS and version being used.
  - Check the box next to the version of UNIX/Linux installed on the asset.
    Note: For UNIX/Linux registration instructions refer to the VMS registration instructions found in the Unix Checklist.
    At the time of this writing, there are no rules within the VMS require the selection additional postures when selecting the UNIX or Linux Operating System.

OR IF the asset is based on a Cisco or Juniper network device OS

- Expand 'Cisco' or 'Juniper' to locate the OS and version being used.
  - Check the box next to the version of OS installed on the asset.
    Note: For Network device registration instructions refer to the VMS registration instructions found in the Network Infrastructure, IP Wan, and/or Backbone Transport Checklists.
    Note: Rules within the VMS MAY require the selection additional postures when selecting a Cisco or Juniper Operating System.

OR IF the asset is based on a embedded network device OS and/or has not been located anywhere else in the OS tree:

- Expand 'Network Device Embedded OS' to locate the OS and version being used.
  - Check the box next to the version of OS installed on the asset.
    Note: For Network device registration instructions refer to the VMS registration instructions found in the Network Infrastructure, IP Wan, and/or Backbone Transport Checklists.
    Note: Rules within the VMS MAY require the selection additional postures when selecting a Network Device Embedded OS. **IF** the appropriate OS has not been located anywhere else in the OS tree, Check the box next to 'Other Network OS'
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.

e) **IF** the asset is a server or a piece of RTS system core equipment, proceed to f) and select all the applications used by the devise as follows;
ELSE skip to "g)" below

f) **Expand 'Application'** to view the available applications. Drill down through the tree to locate all applications and versions being used by the asset. This is a required step to define what applications are installed on the asset for which there is configuration guidance or for which IAVM notices exist. This requirement is typically applicable to RTS core equipment and servers. The SA (or reviewer) is responsible for knowing what general-purpose applications the asset being registered uses or is based upon. The SA (or reviewer) is further responsible for selection all general-purpose applications that the asset being registered uses. The following steps will detail applications that are typically found as the basis of or used by RTS assets.

- **Expand 'Database'** and drill down to find the version of database being used on the asset. If not used or not found; skip this selection.
  - Check the box next to the version of Database being used on the asset.
    Note: For Database registration instructions refer to the VMS registration instructions found in the Database Checklist.
    Note: Rules within the VMS require the selection additional postures when selecting a Database.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.
- **Expand 'Web Server'** and drill down to find the version of Web Server being used on the asset. If not used or not found; skip this selection.
  - Check the box next to the version of Web Server being used on the asset.
    Note: For Web Server registration instructions refer to the VMS registration instructions found in the Web Server Checklist.
    Note: Rules within the VMS require the selection additional postures when selecting a Web Server.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.
- **Expand 'Application Servers'** and drill down to find the version of Application Server being used on the asset. This will typically be a version of Tomcat. If not used or not found; skip this selection.
  - Check the box next to the version of Application Server being used on the asset.
    Note: For Application Server registration instructions refer to the VMS registration instructions found in the Web Server and Application Checklists.

Note: Rules within the VMS require the selection additional postures when selecting an Application Server.

- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **'Save'** again.
- **Expand 'Browsers'** and drill down to find the version(s) of Browser(s) being used on the asset. If not used or not found; skip this selection.
  Note: If a browser was automatically added to the asset's posture when selecting a Windows OS and it is the correct browser, skip this selection. If not, select the proper browser, add it, and select the incorrect browser version and click '<<' to remove it.
  - Check the box next to the version of Browser being used on the asset.
    Note: For Browser registration instructions refer to the VMS registration instructions found in the Web Checklist and/or Desktop Application Checklist.
    Note: Rules within the VMS require the selection additional postures when selecting a Browser.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **'Save'** again.
- **Expand 'Antivirus'** and drill down to find the version of Antivirus being used on the asset. If not used or not found, skip this selection. The use of Antivirus software is a requirement for all Windows based systems.
  - Check the box next to the version of Antivirus being used on the asset.
    Note: For Antivirus software registration instructions refer to the VMS registration instructions found in the Desktop Application Checklist.
    Note: Rules within the VMS MAY require the selection additional postures when selecting Antivirus Software.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
- **Expand 'JVM'** and drill down to find the version of Java Virtual Machine Manager being used on the asset. If not used or not found; skip this selection. This is required, however, when registering certain other web server postures.

  - Check the box next to the version of ESM software being used on the asset.
    Note: For JVM registration instructions refer to the VMS registration instructions found in the Web Server Checklist.
    Note: Rules within the VMS MAY require the selection additional postures when selecting a Java Virtual Machine.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.
- **Expand 'MSdotNETFramework'** and drill down to find the version of Framework being used on the asset. If not used or not found; skip this selection.
  - Check the box next to the version of Framework being used on the asset.
    Note: For dotNET Framework registration instructions refer to the VMS registration instructions found in the Web Server Checklist.
    Note: Rules within the VMS MAY require the selection additional postures when selecting a dotNET Framework.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.
- **Expand 'ESM'** and drill down to find the version of Enterprise System Manager being used on the asset. If not used (not typically used) or not found; skip this selection.
  - Check the box next to the version of ESM software being used on the asset.
    Note: For ESM registration instructions refer to the VMS registration instructions found in the ESM Checklist.
    Note: Rules within the VMS MAY require the selection additional postures when selecting ESM software.
- **Click '>>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the 'Selected' box. Click 'Add'.
- **Click 'Save'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the 'Selected' box.
  - Click **'>>'** and **Save'** again.

- **Expand '<u>Office Automation</u>'** and drill down to find the version of Office Automation software being used on the asset. If not used (not typically used) or not found; skip this selection.
  - Check the box next to the version of Office Automation software being used on the asset.
    <u>Note</u>: For Office Automation registration instructions refer to the VMS registration instructions found in the Desktop Application Checklist.
    <u>Note</u>: Rules within the VMS MAY require the selection additional postures when selecting an Office Automation.
- **Click '<u>>></u>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the '<u>Selected</u>' box. Click '<u>Add</u>'.
- **Click '<u>Save</u>'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the '<u>Selected</u>' box.
  - Click **'<u>>></u>'** and **<u>Save</u>'** again.

g) **IF** registering a network switch, router, or other network transmission element, that is part of a LAN supporting an Adjunct or Auxiliary system or the management of the RTS system or an Adjunct or Auxiliary system, AND it is NOT part of the BCPS LAN/CAN/BAN/WAN network infrastructure or management system, proceed to h) below:
ELSE skip to i) below:

h) Expand '<u>Network</u>' then '<u>Data Network</u>' and refer to the VMS registration instructions found in the Network Infrastructure, IP Wan, and/or Backbone Transport Checklists.
- Check the boxes next to the appropriate postures for the asset.
- **Click '<u>>></u>'** to move the posture to the 'Selected' window (Optional/Recommended)
  - Enter any additional information requested by the appearance of an input box under the '<u>Selected</u>' box. Click '<u>Add</u>'.
- **Click '<u>Save</u>'**. (Optional/Recommended)
  - Satisfy any Rule alert that appears under the '<u>Selected</u>' box.
  - Click **'<u>>></u>'** and **<u>Save</u>'** again.

i) **Click '<u>Save</u>'** one last time Proceed to x.

x. **Click the '<u>Functions</u>' tab** to select the function of the asset being registered.
- Select all functions that the asset performs. If an appropriate function is not found; skip this selection.
- Click '<u>>></u>' to move it to the '<u>Selected</u>' window.
- Click '<u>Save</u>'

xi. **Click the '<u>Systems / Enclaves</u>' tab** to associate this asset with the appropriate or all applicable program(s), enclave(s), and site(s).
- In the '<u>Available Systems</u>' box:
  - Find and select '<u>DISN-DSN</u>' if the system can place or receive DSN calls.

  OR
  - Find and select '<u>DISN-DRSN</u>' if the system can place or receive DRSN calls.

- Click '>>' to move it to the 'Selected Systems' window
- IF the RTS System is managed or monitored by the ADIMSS (DSN), Find and select 'ADIMSS'

OR

- IF the RTS System is managed or monitored by the ARDIMSS or ESRS (DRSN), Find and select 'ARDIMSS' and/or 'ESRS'
- Click '>>' to move it to the 'Selected Systems' window

o In the 'Available Enclaves' box:
- Find and select the local enclave that the RTS system is part of. (i.e., your site/location) (These selections may not in the list as yet)
  Note: For registered enclaves, choose the enclave. If the enclave is not present, your IAM to determine if the enclave has been requested to be added. [*(Reviewer Only)* contact your team lead.] If the team lead or IAM has requested an enclave be added; 'Select Has Been Requested'. If the enclave has not been requested; 'Select Not Available'. There should not be any assets registered/updated that are not part of an enclave.

o Click '>>' to move it to the 'Selected Systems' window
o Click 'Save'

xii. **Click the 'Additional Details' tab** and provide all of the requested information for the RTS asset; Building and room number should reflect the actual location of the RTS of the asset. Other information requested is Serial Number and Barcode, Make, Model and Manufacturer.
xiii. **Click 'Save'**.
xiv. Return to step vi to create another Computing asset or proceed to Reviewing Assets in the next section.

Note: (Reviewer) New assets created by a reviewer will be found under the 'Not Selected for Review" area of the visit tree for the site that the asset is registered to.

Note: (Reviewer) Changing the status of one vulnerability will move the asset from the 'Not Selected for Review" area or the 'Must Review' area to the 'Reviewed" area of the visit tree for the site that the asset is registered to.

Note: When creating a NEW asset it is recommended to run a VL03 report to identify the IAVMs that will be assigned to the new asset being created. (See instructions below). IAVMS that are assigned to an asset will default to an open status and must be acknowledged and fixed immediately. All other vulnerabilities will default to 'Not Reviewed'

Note: The following process may be used in the event that there is a need to create multiple assets having the **same** configuration or postures.
CAUTION: Extreme care must be exercised when performing this procedure. The identifying information MUST be changed (as listed under "minimum edit" below). If this information is not changed, the exported asset will be updated only.

- Create the first asset and save it.

- While displaying the first asset's registration information, export the asset. This will create a .xml file on your computer that contains the registration information.
- Open the .xml file in a text editor.
- Edit the identifying information for the asset.
    - At a minimum edit the following:
        - Asset name
        - Host name
        - Unique ID
        - MAC Address
        - IP address
    - Optionally edit the following:
        - Building
        - Room
        - Serial number
        - Barcode
- Save the edited information insuring that the file name is changed appropriately and the .xml extension is maintained.
- Return to VMS and click the XML icon to the right of the file folder icon nest to computing. Browse for the file and click submit.
- Open the newly created asset and update/validate all identification and posture information. Update as needed.

1.7 Reviewing Assets – Step-by-Step

Note: The AS01 report can assist the review by quickly identifying the assets at the location the review is being performed. This will also identify the assets that have been created and can help to eliminate the creation of duplicate assets (i.e., the same asset under different names) Instructions for generating this report are provided under "Additional Reports" below.

1.7.1 First Review of the Asset under VMSv6

When reviewing an asset for the first time under VMSv6 or after initial registration in VMSv6, all asset registration and posture information must be validated. This occurs under the following conditions.

- The asset had been registered in VMSv5.4 and has been brought forward into VMSv6.
  - Additional information as well as the asset postures must be added.
- An SA has initially registered the asset under VMSv6 and a Reviewer will be performing a review on the asset.
  - The reviewer must validate that all information and applicable postures have been properly assigned to the asset. The reviewer must work with the SA to insure proper and complete registration occurs.

c. Steps

i. **Expand 'Asset Findings Maint'**
ii. **Click 'Assets/Findings'**
iii. ***(SA)*** **Expand 'By Location'** and proceed to step vi.
(Reviewer Only) Expand 'Visits' to display its sub-folders
iv. *(Reviewer Only)* Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
v. *(Reviewer Only)* Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
vi. **Expand 'Computing'**.
vii. *(Reviewer Only)* **Expand 'Must Review'**
SA will not see 'Must Review', but will proceed to step viii.
viii. **Click the 'Asset Name'**.
  - Verify data in 'General' tab and 'Asset Identification'.
    For details see Section 1 "Creating the Asset", steps vii and vii.

ix. **Click the 'Asset Posture' tab** verify the postures/functions assigned to the asset:
  - Expand 'The Asset Name' in the 'Selected ' window (if it's there.)
  - Verify that all postures for the asset has been selected and are accurate.
  - IF the asset is not shown in 'Selected' box, or the postures are not accurate, see Section 1 "Creating the Asset", step ix.
    Note: Assets registered under VMSv5.4 may have an OS assigned, but the additional postures/functions will have to be assigned.

x. **Click the 'Functions' tab**

- Verify that all Functions for the asset has been selected and are accurate. See Section 1 “Creating the Asset”, step x. (As of 4/7/06 there are no RTS specific functions. This step may be skipped at this time.)

xi. **Click the ‘Systems / Enclaves’ tab**.
- Verify that the asset has been associated with the appropriate or all applicable program(s), enclave(s), and site(s). See Section 1 “Creating the Asset”, step xi.

xii. **Click the ‘Additional Details’ tab**
- Verify that the information on this tab is accurate. See Section 1 “Creating the Asset”, step xii.

xiii. If any of the information found is inaccurate, See Section 1 “Creating the Asset” for instructions on making additions or changes.

xiv. Continue with the following section ‘Procedures for Review of the Asset’ step vii ‘Must Review’

1.7.2 Procedures for Updating the Vulnerability Status of the Asset

If all registration tasks have been accomplished and/or verified, use the following procedures for updating the status of all assets, both computing and non-computing:
Note: (*Reviewer Only*) In the event that the Voice/Video/RTS asset just reviewed does not exist in VMS, the reviewer may create it. It is highly recommended that the reviewer have the Voice/Video/RTS SA create the asset and then work with him/her to assure that the asset is fully and properly registered and named or identified in accordance with the Voice/Video/RTS asset registration instructions described above. If a reviewer must create an arbitrary asset to enter his/her vulnerability statuses, he/she must notify the team lead, others on the team that may also have to update their statuses on the same asset, and the Voice/Video/RTS asset SA. The Voice/Video/RTS asset SA may then update the registration information as needed. Additionally, the reviewer should check with the Voice/Video/RTS asset SA before creating a new asset in the event that the asset does exist in VMS but shows up in a different part of VMS. (i.e., identified differently or registered to a different organization). If a reviewer creates an asset, he/she becomes the SA or "owner" for the asset. "Ownership" of assets created by a reviewer must be transferred to the actual SA for the asset.

d. *Steps*
   i. **Expand 'Asset Findings Maint'**
   ii. **Click 'Assets/Findings'**
   iii. ***(SA)*** **Expand 'By Location'** and proceed to step vi.
   (Reviewer Only) Expand 'Visits' to display it's sub-folders
   iv. *(Reviewer Only)* Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.
   v. *(Reviewer Only)* Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
   vi. **Expand 'Computing'** and/or **'Non-Computing' and/or 'CNDS'** as applicable
   vii. *(Reviewer Only)* **Expand 'Must Review'**
   SA will not see 'Must Review', but will proceed to step viii.
   Note: (*Reviewer Only*) Newly created assets will appear under "Not Selected for Review".
   viii. **Expand the ' Asset Name'** for the asset to be reviewed. The icon in front of "Ready to review" assets is colored in RED. Drill down until the list of vulnerabilities displays under the asset. If multiple postures were selected for the asset during registration, a list of the postures is displayed. Expand each posture to see the list of vulnerabilities under each.
   Note: Determine what postures, if any, can be reviewed and updated using automation. This would apply to any posture / technology for which a Gold Disk or a set of review scripts exist. (i.e., Windows Gold disk(s), and scripts for Unix, Database, and Web Servers). It is highly recommended that this automation be used to review as many findings as possible before beginning a manual review or update of the remaining vulnerabilities. Once reviewed in this manner, the results are imported into VMS to update the status of the vulnerabilities for each set of automation or technology. All vulnerabilities may be updated manually.

Note: To review / update all vulnerabilities under all major postures or technologies other than Voice/Video/RTS, Refer to the Asset Review instructions found in the appropriate checklist for that technology.
Note: When you drill down into the lowest level of the asset tree, you will find the Vulnerabilities and IAVMs assigned to the asset.

ix. **Click on a 'Vulnerability Key'** in the tree that needs to be updated to open its status update area and tabs (scroll down to see if necessary).
x. **On the 'Status' Tab**, Update the 'Status' of the vulnerability.
Note: If selecting a status of 'O-Open', a 'Details' and 'Milestone' must also be entered.
xi. **Click the 'Details' Tab**, (Conditional) identify details on all open vulnerabilities/findings by adding to or modifying the default details displayed in the box.
xii. **Click the 'Comments' Tab**, (Optional) Add ,any pertinent comments
xiii. **Click the 'Programs' Tab**, (Conditional)
Note: This is a place holder for future instructions relating to Program Baselines
xiv. **Click the 'POA&M' Tab**, (*SA, not Reviewer*) (Conditional)
Note: SAs performing self-assessments are required to enter a POA&M for all open vulnerabilities/findings before the status will save. This does not apply to a reviewer.
- Click the 'New Milestone' Button, Enter a 'Milestone' (description of a step in mitigating/fixing the finding) and a 'Completion Date'.
- Click the 'Disk/Save' icon on the left to save the milestone
- Enter additional milestones as necessary.

xv. **Click the 'Apply to Other Findings' Tab**, (Conditional) If applicable: Check 'Choose Other Assets with the Same Finding in the Same Status'. Select the appropriate assets.
Note: If this feature of VMS is to be used, it must be used before clicking 'Save' or else no assets with similar postures / statuses will be found.
xvi. **Click the 'Save'** button at the bottom of the form area
Note: Alert messages will be shown below the 'Save' Button. If alert messages display, the status update information will not save until the alert message(s) is satisfied.
xvii. Return to step ix above and select another 'Vulnerability Key'. Repeat this until all 'Computing' and 'Non-Computing' asset vulnerability statuses are updated.
Note: System Administrators should expand the OS assigned to the asset and each IAVM. Verify the OS level meets the required release or patch level.

1.7.3 Verify that all necessary assets were reviewed

e. Steps

i. **Expand 'Asset Findings Maint'**
ii. **Click 'Assets/Findings'**
iii. ***(SA)*** **Expand 'By Location'** and proceed to step vi.
(Reviewer Only) Expand 'Visits' to display it's sub-folders
iv. *(Reviewer Only)* Expand the sub-folder you are assigned. Each subfolder represents an individual visit in VMS that has been assigned for your review.

v. *(Reviewer Only)* Expand the visit and display the location summaries for the visit. Within the location, assets are divided into computing, non-computing and CNDS.
vi. **Expand 'Computing'** and/or **'Non-Computing' and/or 'CNDS'** as applicable
vii. *(Reviewer Only)* **Expand 'Must Review'**
SA will not see 'Must Review', but will proceed to step viii.
viii. **Expand Each 'Asset Name'** to view the list of asset postures.
o If checkmarks are gone, the asset has been fully reviewed.
ix. **Done**

The following reports can be used to verify the status of the site and its assets.

1. VC06 Asset Compliance Report
    a. A Full report may be obtained
2. VC03 Severity Summary Report
    a. Table of numbers only
3. VC01
    a. Used for IAVM Compliance

See **Compliance monitoring** below for a quick set of instructions on generating these reports.

1.7.4 Add Comments to a Visit (Reviewer only)

f. Steps– Click the following:
i. 'Visit Maint.'
ii. Expand the Organization the visit is set up for.
iii. Expand the Visit
iv. Locate the visit you are working on. (Drill down till you find it)
v. Click on CCSD or enclave name. (Drill down till you find it)
vi. 'Comments Tab'
    a) Type your comments
vii. 'Save Changes'

1.8 Reports – Step-by-Step

1.8.1 Compliance Monitoring

- **VC06** – provides a detailed report of all vulnerabilities that are assigned to an asset and its postures. There are many items that can be selected for display and the report can be filtered and sorted in multiple ways.
  g. Steps– Click the following:
    i. 'Reports'
    ii. 'VC06'
    iii. Select an 'Asset(s)' or an 'Organization(s)'.
    iv. Select "open" status to see only "Open" findings (Select others as desired. Hold the Ctrl or Shift key to make multiple selections)
    v. Select the sort order under 'Sort By'
    vi. Select the information to be displayed: Check the following boxes:
        4. 'Finding Comments'
        5. 'Finding Long Name' (Because it's truncated otherwise)
        6. 'Finding Details'
        7. 'Vulnerability Discussion'
        8. Others as desired
    vii. 'Generate Report'

- **VC03** – Provides a table of assets and technologies with the number and percentage of findings against each listed by severity category. Has numbers only.
  a. Steps– Click the following:
    i. 'Reports'
    ii. 'VC03'
    iii. Select an 'Organization(s)'
    iv. Review other options and select as desired
    v. 'Generate Report'

- **VC01 -** Used for IAVM Compliance (An SA may not see this option)
  a. Steps– Click the following:
    i. 'Reports'
    ii. 'VC01'
    iii. On the 'Organizations' Tab, Select an organization
    iv. On the 'Vulnerabilities' Tab, Select IAVM(s) or year(s)
    v. Review other options and select as desired
    vi. 'Generate'

1.8.2 Additional Reports

The following reports can be used for identifying assets at a site or location and determine what IVAMs are related to specific assets. Quick step by step instructions for creating the reports follows.

- **AS01 - Identifying Assets**
  Note: The AS01 report can assist the review by quickly identifying the assets at the location the review is being performed. These instructions are applicable to locating all assets but are geared toward Telecom/RTS assets.
  a. Steps – Click the following:
    i. 'Reports'
    ii. 'AS01'
    i. Select 'Computing', hold Ctrl key, and select 'Non-Computing' (SUBMIT)
    ii. Select 'By Location' (SUBMIT)
    iii. Select the location
      1. May want to do other reports if your site manages or owns assets that are not located at their site. Check the box for Child Locations if applicable. (SUBMIT)
    iv. Expand 'Non-Computing'
      1. Check the box for 'Telecom Policy'
    v. Expand 'Computing'.
      1. Check the box for 'Telecom'
    vi. Select 'Online', 'Offline', or 'Both'. Located under the right calendar ('Both' is recommended but 'Online' is the default)
    vii. Check the box for 'Show Detailed Asset Information' (Recommended - This will show a tree display of all postures that have been assigned to the asset during registration)
    viii. Check the box for 'Show System Administrator Information' (Recommended)
    ix. Submit to receive the Telecom/RTS Asset Report
    Note: Reports are best displayed using the 'Output / Screen' option. The display may then be printed. Clicking the IE6 print function prints the report only without the surrounding frames. Using the 'Output / Export file' option produces a tab delimited text file. This file can be opened with excel to receive a database like table of the information. Use Right Click/Open With in Windows to open the file.

- **VL03 - Look at IAVMs assigned to an Operating System or Application**
  Note: The VL03 report can assist the review by quickly identifying the IAVMs that will be identified to the asset when you select the operating system of the asset. This can be accomplished by performing the following steps.
  a. Steps– Click the following:
    i. 'Reports'
    ii. 'VL03'
    x. Select 'Select by Operating System/Application(s)'
    xi. Select the OS(s) and Applications(s) to report on

xii. Select the environment (SUBMIT)
xiii. Select any additional display options or deselect the default selections
iii. 'Generate Report'

DSN01.01 V0007921 CAT III The IAO does not conduct self-inspections

8500.2 IA Control: ECMT-1, ECMT-2, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.1

Vulnerability The IAO does not conduct and document self-inspections of the DSN components at least semi-annually for security risks.

Checks

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

Fixes

Perform self-inspections

Establish policy and procedures to ensure that, at a minimum, semi-annual security self-inspections are conducted.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN01.02 V0007922 CAT III Switch usage is not monitored for security

8500.2 IA Control: ECMT-2, ECMT-1, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.1

Vulnerability The sites telephone switch is not frequently monitored for changing calling patterns and system uses for possible security concerns.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN01.03 V0007923 CAT II Inadequate clearance / access to perform duties

8500.2 IA Control: ECLP-1, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.1

Vulnerability The ISSO/IAO does not ensure that administration and maintenance personnel have proper access to the facilities, functions, commands, and calling privileges required to perform their job.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Fixes

Provide necessary Privileges/A

The ISSO/IAO should Implement appropriate processes, local policies, and/or procedures to provide maintenance personnel and SAs with the appropriate access and system privileges needed to properly perform their tasks and responsibilities

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN02.01 V0007924 CAT III DSN systems are not registered in the DISA VMS

8500.2 IA Control: ECND-1, ECND-2, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.3

Vulnerability DSN systems are not registered in the DISA VMS

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Validate VMS Registration

In VMS, validate that the (all) assets and their SAs are required to be registered that are required to be registered.

Fixes

Comply with policy - VMS Regi

Comply with policy. Register all assets and their SAs in the DISA/DoD VMS that are required to be registered.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN02.02 V0007925 CAT III DSN SAs are not registered with the DISA VMS

8500.2 IA Control: ECND-2, ECSC-1, ECND-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.3

Vulnerability System Administrators (SAs) responsible for DSN information systems are not registered with the DISA VMS.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Validate VMS Registration

In VMS, validate that the (all) assets and their SAs are required to be registered that are required to be registered.

Fixes

Comply with policy - VMS Regis

Comply with policy. Register all assets and their SAs in the DISA/DoD VMS that are required to be registered.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN02.03 V0007926 CAT II IAVAs are not responded to in the specified time

8500.2 IA Control: ECND-2, ECSC-1, ECND-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.2

Vulnerability The ISSO/IAO and ISSM/IAM, in coordination with the SA, will be responsible for ensuring that all IAVM notices are responded to within the specified time period.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Fixes

Comply with policy - IAVM

Comply with policy. The ISSM/IAM/IAO will establish a policy to ensure that IAVMs are being acknowledged, implemented, and closed, in accordance with DOD policy. SAs will update affected systems in accordance with the IAVM recommendations. The ISSM/IAM/IA

Comply with policy - IAVM / Ve

Comply with policy. Contact the VoIP system vendor upon receipt of a IAVA to determine if the vendor can provide the required approved patch or refer the IAVA to the vendor for testing and approval

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN02.04 V0008338 CAT II Vendor Patches not used to close IAVMs

8500.2 IA Control: ECND-2, ECSC-1, ECND-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG SECTION 3.1.2

Vulnerability IAVMs are not addressed using RTS system vendor approved or provided patches.

Checks

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Fixes

Comply with policy - IAVM

Comply with policy. The ISSM/IAM/IAO will establish a policy to ensure that IAVMs are being acknowledged, implemented, and closed, in accordance with DOD policy. SAs will update affected systems in accordance with the IAVM recommendations. The ISSM/IAM/IA

Only apply vendor-approved pa

Only Apply vendor-approved or vendor supplied patches. Correct site policy to require only vendor provided and approved patches are applied.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN02.05 V0008339 CAT III DoD RTS/IS vulnerabilities NOT managed with a VMS

8500.2 IA Control: ECSC-1, ECND-2, ECND-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.3

Vulnerability DoD voice/video/RTS information system assets and vulnerabilities are not tracked and managed using any vulnerability management system as required by DoD policy.

Checks

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN03.01 V0008340 CAT III Voice/Video/RTS system/device NOT STIG compliant

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.4

Vulnerability A DoD Voice/Video/RTS system or device is NOT configured in compliance with all applicable STIGs or the appropriate STIGs have not been applied to the fullest extent possible.

Checks

Review SRR Results - All Appli

Obtain a copy of all applicable SRR or Self Assessment results and review for compliance OR perform all applicable SRRs on a representative number of RTS systems and devices. If there are a significant number of findings reported or if an applicable STIG was not applied, this is a finding.
Note: The specific Voice/Video/RTS system server or device determines the applicability of any given STIG. Many Voice/Video/RTS system servers or devices are based on general-purpose operating system such as Microsoft Windows, Unix, or Linux. They may use general-purpose applications such as databases like MS-SQL or Oracle and/or employ web server technology like IIS or similar. Determine what the system under review is based upon and perform the associated SRRs. Additionally, an application SRR may be applicable for the vendor's application that makes the server or device perform the functions or the management of the system.
Note: Voice/Video/RTS systems and devices are required to be tested, certified, accredited by the DSAWG and listed on the DSN APL. Each specific Voice/Video/RTS system or device may be approved while having certain open findings that are approved in light of certain mitigations. Such open findings are not to be considered in the status determination of this requirement.

Fixes

Apply STIG(s) - All applicable

The IAO and/or SA is to configure all Voice/Video/RTS systems, server, and devices in accordance with all applicable STIGs for the specific system/server/device while taking into account any DSAWG approved open findings and their mitigations.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN03.02 V0008341 CAT III "STIG Compliance" not required in contracts

8500.2 IA Control: ECSC-1, EBCR-1, DCAS-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.4

Vulnerability The purchase / maintenance contract, or specification, for the Voice/Video/RTS system under review does not contain verbiage requiring compliance and validation measures for all applicable STIGs.

Checks

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN03.03 V0008342 CAT IV "STIG Compliance" in contracts NOT enforced

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.4

Vulnerability The DAA, IAM, IAO, or SA for the system DOES NOT enforce contract requirements for STIG compliance and validation

Checks

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Fixes

Enforce Contract Requirements

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN03.04 V0008345 CAT II A RTS system is in use but is NOT DSN APL listed

8500.2 IA Control: ECSC-1, EBCR-1, DCAS-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.5

Vulnerability A Voice/Video/RTS system is in operation but is not listed on the DSN APL nor is it in the process of being tested.

Checks

Comply with Policy - DSN APL

Verify that the VoIP system is listed on the DSN APL by checking at the following link: http://jitc.fhu.disa.mil/tssi/apl.html If not, contact the VCAO to determine if the system is in the testing process.

Fixes

Comply with Policy - DSN APL

Ensure non-certified VoIP systems are not connected to the DSN. Sponsor the system for DSN APL testing and certification.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN03.05 V0008346 CAT III RTS system NOT installed according to restrictions

8500.2 IA Control: DCAS-1, EBCR-1, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.5

Vulnerability A Voice/Video/RTS system or device is NOT installed according to the deployment restrictions and/or mitigations contained in the IA test report, Certifying Authority's recommendation and/or DSAWG approval documentation.

Checks

Inspect or Review Documents

Or review the required "documents on file" that are necessary for compliance with the requirement.

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

Comply with Policy - Deploymen

Comply with policy. Comply with the deployment limitations and/or installation restrictions and open vulnerability mitigations contained in the DSN APL IA final testing report generated by the VCAO after DSAWG approval.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN03.06 V0008347 CAT IV A RTS system is not implemented as APL listed

8500.2 IA Control: DCAS-1, EBCR-1, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.5

Vulnerability A Voice/Video/RTS system or device is NOT installed in the same configuration and being used for the same purpose that was tested for prior to DSAWG approval and DSN APL listing.

Checks

Inspect or Review Documents

Or review the required "documents on file" that are necessary for compliance with the requirement.

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Fixes

Comply with policy – Solution

Comply with policy. Comply with the solution configuration as tested and contained in the DSN APL IA final testing report generated by the VCAO after DSAWG approval.

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN03.07 V0008348 CAT IV DSN APL not considered during procurement

8500.2 IA Control: EBCR-1, DCAS-1, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.5

Vulnerability The requirement of DSN APL listing is not being considered during the procurement, installation, connection, or upgrade to the site's Voice/Video/RTS infrastructure.

Checks

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Fixes

Comply with Policy - DSN APL

Ensure non-certified VoIP systems are not connected to the DSN. Sponsor the system for DSN APL testing and certification.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN04.01 V0007930 CAT II Management terminals not on a dedicated LAN

8500.2 IA Control: ECSC-1

References: Defense Switched Network (DSN) STIG V1R1 Sect. 4.3

Vulnerability Switch administration, ADIMSS, or other Network Management terminals are not located on a dedicated LAN.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Fixes

Establish segregated mgmt LAN

The ISSO/IAO will ensure that all DSN Network Management, switch administration components and other authorized systems are connected to a dedicated network and prohibit all connections to the ADMISS or other Network Management network that are not releva

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN04.02 V0007931 CAT II No IP or packet filtering on NMS routers

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.3

Vulnerability Network Management routers located at switch sites are not configured to provide IP and packet level filtering/protection.

Checks

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

> Review current configuration

> Review current configuration files of effected devices to confirm compliance.

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Limit access using router AC

> Limit access to the telecom switch and other management devices by providing IP and packet level filtering/protection on the router through the use of an ACL that restricts access to/from known IP addresses that are permitted to connect to the system d

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN04.03 V0007932 CAT II Admin terminals are used for day-to-day apps

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.2

Vulnerability Administration terminals are used for other day-to-day functions (i.e. email, web browsing, etc).

Checks

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Dedicate admin terms to admi

Ensure dedicated terminals and workstations are used to administer DSN switching systems to that purpose only. Do not administer DSN switching systems from computer terminals that are used for day-to-day functions (i.e. email, web browsing, etc).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN04.04 V0007933 CAT II Admin terms not on a segregated connection

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.2

Vulnerability Switch Administration terminals do not connect directly to the switch administration port or connect via a controlled, dedicated, out of band network used for switch administration support.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Segregate admin term connect

Insure that the connections used are through either a dedicated out of band network or direct connection to the administration port. Any other connections to administration ports or OOB networks should be disconnected and their use should be discontinued.

Segregate admin term connectio

Ensure that the connections used are through either a dedicated out of band network or direct connection to the administration port. Any other connections to administration terminals should be disconnected and their use should be discontinued.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN04.05 V0007934 CAT III Attendant ports available to unauthorized users

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.2.1.2

Vulnerability Attendant console ports are available to unauthorized users by not allowing any instrument other than the Attendant console to connect to the Attendant console port.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN04.06 V0007935 CAT III The ISSO/IAO has not established SOPs

8500.2 IA Control: DCSW-1, DCID-1, ECSC-1, DCSD-1, DCHW-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.6.1

Vulnerability The ISSO/IAO has not established Standard Operating Procedures.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Inspect or Review Documents

Or review the required “documents on file” that are necessary for compliance with the requirement.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

Develop SOPs

The ISSO/IAO should develop an SOP that will satisfy the requirements as outlined in the DSN STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN04.07 V0008545 CAT II OAM&P/NM and CTI networks are NOT dedicated / OOB

8500.2 IA Control: ECSC-1, EBCR-1, DCPA-1, DCID-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.2

Vulnerability OAM&P / NM and CTI networks are NOT dedicated to the system that they serve in accordance with their separate DSN APL certifications.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN04.08 V0008544 CAT II OAM&P/NM / CTI LAN is connected to general use LAN

8500.2 IA Control: ECSC-1, EBCR-1, DCPA-1, DCID-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.2

Vulnerability An OAM&P / NM and CTI network/LAN is connected to the local general use (base) LAN without appropriate boundary protection.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN04.09 V0008542 CAT II OAM&P/NM / CTI LAN is connected to general use LAN

8500.2 IA Control: ECSC-1, EBCR-1, DCID-1, DCPA-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.2

Vulnerability An OAM&P / NM and CTI network/LAN is connected to the local general use (base) LAN without appropriate boundary protection.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN04.10 V0008541 CAT II An OAM&P / NM or CTI network NOT STIG compliant

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.2

Vulnerability An OAM&P / NM or CTI network DOES NOT comply with the Enclave and/or Network Infrastructure STIGs.

Checks

> Review SRR Results - Net/Enc

Obtain a copy of Network and Enclave SRRs or Self Assessment results and review for compliance OR perform Network and Enclave SRRs on the OAM&P / NM and/or CTI network. If there are a significant number of findings reported or if an applicable STIG was not applied, this is a finding.

Note: Voice/Video/RTS and/or OAM&P / NM and/or CTI network systems and devices are required to be tested, certified, accredited by the DSAWG and listed on the DSN APL. Each specific Voice/Video/RTS system or device may be approved while having certain open findings that are approved in light of certain mitigations. Such open findings are not to be considered in the status determination of this requirement.

Fixes

> Apply STIG(s) – Network/Encl

Configure all OAM&P / NM or CTI networks in accordance with the Enclave and Network Infrastructure STIGs while taking into account any DSAWG approved open findings and their mitigations for the given solution.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN05.01 V0007936 CAT II Security packages have not been installed

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.2.1.1

Vulnerability Applicable security packages have not been installed on the system.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

Fixes

Apply security packages

Apply all required security software to the DSN components as required.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN06.01 V0007937 CAT II Improper oversight of Foreign Nationals

8500.2 IA Control: ECSC-1, PECF-1

References: Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation Table E3.T1., DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.9.1

Vulnerability The IAO DOES NOT ensure that all temporary Foreign/Local National personnel given access to DSN switches and subsystems for the purpose of installation and maintenance, are controlled and provided direct supervision and oversight (e.g., escort) by a knowl

Checks

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN06.02 V0008519 CAT II FN/LN personnel NOT properly cleared

8500.2 IA Control: PECF-1, ECAN-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.9.1

Vulnerability Foreign/Local National personnel hired by a base/post/camp/station for the purpose of operating or performing OAM&P / NM functions on DSN switches and subsystems have not been vetted through the normal process for providing SA clearance as dictated by the

Checks

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Fixes

Obtain DD Form 2875- all users

Obtain a System Authorization Access Request (SAAR) DD Form 2875 for each DRSN user to validate their need-to-know

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN06.03 V0008520 CAT II FN/LN personnel have improper access/duties

8500.2 IA Control: PECF-1, ECAN-1

References: DODI 8100.3; Department of Defense (DoD) Voice Networks , DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.9.1.1

Vulnerability Foreign/Local National personnel have duties or access privileges that exceed those allowed by DODI 8500.2 E3.4.8.

Checks

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN06.04 V0007940 CAT IV Access based on duty hours is available & NOT used

8500.2 IA Control: ECSC-1, ECLO-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.2

Vulnerability The option to restrict user access based on duty hours is available but is not being utilized.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> DSN06.04 -Use TOD access res

If the time of day (TOD) access restriction function is available through the DSN system, it should be provisioned to allow user access within a specified window. For example, if a user is assigned to work on a DSN component Monday through Friday 8 am –

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN06.05 V0008558 CAT II SA account privileges are not limited per duties

8500.2 IA Control: ECSC-1, ECLP-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.9.1

Vulnerability System administrative and maintenance users are assigned accounts with privileges that are not commensurate with their assigned responsibilities.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

>> DSN06.05

Verify each SA's and maintenance person's required access level; Within the system determine system user access levels assigned to each user and ensure that not all switch techs have super user access.

>> DSN06.05 - NORTEL

Request and review "Show Users" on switch.

>> DSN06.05 - Siemens

Request and Review "DISPUSERID" on Switch

>> DSN06.05 - Tekelec

Request and Review 'rtrv-secu-user' on STP

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> DSN06.05 Ensure Least Privi

Review and evaluate all user accounts and assign privileges to DSN system components and ensure access level assignment is commensurate to the users job function.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN06.06 V0008556 CAT III SA and maintenance user accounts NOT documented

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.2

Vulnerability All system administrative and maintenance user accounts are not documented.

Checks

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

> Inspect/Review Documents

Inspect or review the required “documents on file” that are necessary for compliance with the requirement.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN06.07 V0008554 CAT III Command classes or command screening NOT used

8500.2 IA Control: ECLP-1, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.2

Vulnerability The available option of Command classes or command screening is NOT being used to limit system privileges

Checks

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN07.01 V0007941 CAT III Direct Inward System Access not controlled

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.2.1.4

Vulnerability The Direct Inward System Access feature and/or access to Voice Mail is not controlled by either class of service, special authorization code, or PIN.

Checks

> Review current configuration

Review current configuration files of effected devices to confirm compliance

Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN07.02 V0007942 CAT III DISA access codes are not changed semi-annually

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.2.1.4

Vulnerability Direct Inward System Access and Voice Mail access codes are not changed semi-annually.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN07.03 V0007943 CAT III Service access codes not changed like passwords

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.2.1.4

Vulnerability Personal Identification Numbers (PIN) assigned to special subscribers used to control Direct Inward System Access and Voice Mail services are not being controlled like passwords and deactivated when no longer required.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN07.04 V0007944 CAT III Service access PINs NOT changed when compromised

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.2.1.4

Vulnerability Privilege authorization, Direct Inward System Access and/or Voice Mail special authorization codes or individually assigned PINS are not changed when compromised..

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN08.01 V0007945 CAT IV Emergency equipment NOT clearly identified/marked

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.11

Vulnerability Equipment, cabling, and terminations that provide emergency life safety services such as 911 (or European 112) services and/or emergency evacuation paging systems are NOT clearly identified and marked.

Checks

> Inspect effected devices

Inspect a sampling of effected devices and confirm compliance

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

DSN08.01 – Label emergency ser

Label all equipment, DS-1 circuit packs. T-1 cross connect ports, cables, termination points, etc that handles Emergency 911 (112) and/or emergency evacuation paging systems. Additionally make all SAs and maintenance personnel working near such equipment

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN08.02 V0008537 CAT IV No emergency announcement system

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.11

Vulnerability There is no system installed that can provide emergency life safety or security announcements

Checks

> Perform a walk through

Perform a walk through of the facility and confirm compliance via inspection of the effected devices or items

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN08.03 V0008539 CAT II NO policy for unclassified RTS in classified areas

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.12

Vulnerability A policy is NOT in place and/or NOT enforced regarding the use of unclassified telephone/RTS instruments located in areas or rooms where classified meetings, conversations, or work normally occur.

Checks

Inspect or Review Documents

Or review the required “documents on file” that are necessary for compliance with the requirement.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN08.04 V0008543 CAT II RTS devices located in SCIFs NOT policy compliant

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.12

Vulnerability Voice/Video/RTS devices located in SCIFs do not prevent on-hook audio pick-up and/or do not have a speakerphone feature disabled or are not implemented in accordance with DCID 6/9 or TSG Standard 2.

Checks

Inspect or Review Documents

Or review the required “documents on file” that are necessary for compliance with the requirement.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN09.01 V0007946 CAT IV SS7 links not identified and routed separately

8500.2 IA Control: ECSC-1

References: Defense Switched Network (DSN) STIG V1R1 Sect. 5.2

Vulnerability SS7 links are not clearly identified and routed separately from termination point to termination point.

Checks

> Perform a walk through

Perform a walk through of the facility and confirm compliance via inspection of the effected devices or items

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

DSN09.01 -Label and separatel

The ISSO/IAO should ensure labeling of all cabling that carries signaling within the facility that houses the DSN component. Labeling should be visible to maintenance personnel and should be spaced no more than 10 feet apart. Path “A” and path “B” signal

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN09.02 V0007947 CAT IV SS7 termination blocks are not clearly identified

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.2.3

Vulnerability The SS7 termination blocks are not clearly identified at the MDF.

Checks

> Perform a walk through

Perform a walk through of the facility and confirm compliance via inspection of the effected devices or items

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

DSN09.01 -Label and separatel

The ISSO/IAO should ensure labeling of all cabling that carries signaling within the facility that houses the DSN component. Labeling should be visible to maintenance personnel and should be spaced no more than 10 feet apart. Path “A” and path “B” signal

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN09.03 V0007948 CAT IV Power cabling serving SS7 equipment not diverse

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.2.3

Vulnerability Power cabling that serves SS7 equipment is not diversely routed to separate Power Distribution Frames (PDF) and identified.

Checks

> Perform a walk through

Perform a walk through of the facility and confirm compliance via inspection of the effected devices or items

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

Route power distribution diver

Label the termination points and fuse positions of power cabling that provides power to signaling equipment. A and B feed power cabling should be routed separately between the signaling frame and the power distribution frame. Power cabling paths that ar

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN09.04 V0007949 CAT IV SS7 Power cabling is NOT clearly marked

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.2.3

Vulnerability Power cabling that serves SS7 equipment is not clearly identified at both the termination point and at the fusing position.

Checks

> Perform a walk through

Perform a walk through of the facility and confirm compliance via inspection of the effected devices or items

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

Label SS7 power distribution

Label the termination points and fuse positions of power cabling that provides power to signaling equipment. A and B feed power cabling should be routed separately between the signaling frame and the power distribution frame. Power cabling paths that ar

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN09.05 V0007950 CAT II Links within the SS7 network are not encrypted.

8500.2 IA Control: ECCT-1, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.2.3

Vulnerability Links within the SS7 network are not encrypted.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

Encrypt SS7 links

Ensure all SS7 links are, at a minimum, bulk encrypted before leaving the facility or installation.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN10.01 V0007951 CAT II VoIP system not JITC certified

8500.2 IA Control: ECSC-1

References: Defense Switched Network (DSN) STIG V1R1 Sect. 6

Vulnerability The ISSO/IAO will ensure that no VoIP systems or networks are connected to the DSN switching system without being certified by the JITC.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Fixes

JITC certify the VoIP system

Ensure non certified VoIP systems are not connected to the DSN.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN10.02 V0007952 CAT II VoIP system/Network NOT STIG compliant

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 4

Vulnerability A DoD VoIP system, device, or network is NOT configured in compliance with all applicable STIGs or the appropriate STIGs have not been applied to the fullest extent possible.

Checks

> Review SRR Results - All App

> Obtain a copy of all applicable SRR or Self Assessment results and review for compliance OR perform all applicable SRRs on a representative number of RTS systems and devices. If there are a significant number of findings reported or if an applicable STIG was not applied, this is a finding.

Note: The specific Voice/Video/RTS system server or device determines the applicability of any given STIG. Many Voice/Video/RTS system servers or devices are based on general-purpose operating system such as Microsoft Windows, Unix, or Linux. They may use general-purpose applications such as databases like MS-SQL or Oracle and/or employ web server technology like IIS or similar. Determine what the system under review is based upon and perform the associated SRRs. Additionally, an application SRR may be applicable for the vendor's application that makes the server or device perform the functions or the management of the system.

Note: Voice/Video/RTS systems and devices are required to be tested, certified, accredited by the DSAWG and listed on the DSN APL. Each specific Voice/Video/RTS system or device may be approved while having certain open findings that are approved in light of certain mitigations. Such open findings are not to be considered in the status determination of this requirement.

Fixes

> Apply STIG(s) - All applicab

> The IAO and/or SA is to configure all Voice/Video/RTS systems, server, and devices in accordance with all applicable STIGs for the specific system/server/device while taking into account any DSAWG approved open findings and their mitigations..

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN11.01 V0007953 CAT II Transport circuits are not encrypted.

8500.2 IA Control: ECSC-1, ECCT-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.2.3

Vulnerability Transport circuits are not encrypted.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

Bulk encrypt all trunks

Bulk encrypt all trunking circuits leaving and entering the DSN switching facility of installation.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN11.02 V0007954 CAT III Physical access to commercial ADM not restricted

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.2.3

Vulnerability Physical access to commercial Add/Drop Multiplexers (ADMs) is not restricted.

Checks

Perform a walk-through - Physi

Perform a walk through of the facility to confirm that all DSN core and transmission devices that are part of the system are located in a secure room or locked cabinet.

Fixes

> Apply physical security

> Take measures to apply or install or upgrade physical security for system core assets (Switches, Servers,) and transmission devices (network switches, routers, muxes, devices). Limit, control, and document the distribution of keys to access the equipmen

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN12.01 V0007955 CAT III The ISSO/IAO does not maintain a security library

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.7

Vulnerability The ISSO/IAO does not maintain a library of security documentation.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Inspect or Review Documents

Or review the required “documents on file” that are necessary for compliance with the requirement.

Fixes

Maintain a security library

Obtain the above mentioned documents and make them available to users, administrators, maintainers, and managers associated with the DSN.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.01 V0007956 CAT II Users do not change their password at first logon

8500.2 IA Control: IAIA-2, IAIA-1, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1

Vulnerability Users are not required to change their password during their first session.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

>> DSN13.01

If the device or system cannot automatically enforce the requirement, attempting to log in under the username/password the ISSO/IAO issued to a random sampling of users that have been issued passwords.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.02 V0007957 CAT I Default accounts and passwords still exist

8500.2 IA Control: IAIA-2, ECSC-1, IAIA-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1, Chairman Of The Joint Chiefs Of Staff Instruction (CJCSI) 6215.01B; Policy For Department Of Defense Voice Networks C-A-4, Para 16

Vulnerability Default passwords and user names have not been changed.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

> Review current configuration files of effected devices to confirm compliance.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

> DSN13.02

Attempt to log onto the system using well-known system and vendor default accounts and passwords. If successful, this is a finding.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Delete default accts / pswds

Delete / change default accts and passwords - Check the component or system for default vendor accounts and passwords. If possible, delete or rename the account and change the default password.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.03 V0007958 CAT II Shared user accounts are used and not documented.

8500.2 IA Control: IAIA-1, IAIA-2, ECSC-1

References: Chairman Of The Joint Chiefs Of Staff Instruction (CJCSI) 6215.01B; Policy For Department Of Defense Voice Networks C-A-1, Para 3, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1

Vulnerability Shared user accounts are used and not documented by the ISSO/IAO.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices.

> Review current configuration

> Review current configuration files of effected devices to confirm compliance.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

>> DSN13.03 - Nortel

> Show Users – Refer to the Nortel appendix to this STIG for more information

>> DSN13.03 - Siemens

DISPUSERID – Refer to the Siemens appendix to this STIG for more information

> DSN13.03 - Tekelec

rtrv-secu-user – Refer to the STP appendix to this STIG for more information

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Document shared accounts

Document shared accounts - i.e., Keep a record of the human user and their assigned username. Shared accounts will only be used if required out of operational necessity and documented by the ISSO/IAO.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.04 V0007959 CAT III Inactive accounts not disabled after 30 days

8500.2 IA Control: ECSC-1, IAIA-1, IAIA-2

References: Chairman Of The Joint Chiefs Of Staff Instruction (CJCSI) 6215.01B; Policy For Department Of Defense Voice Networks C-A-5, Para 18-c, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1

Vulnerability The option to disable user accounts after 30 days of inactivity is not being used.

Checks

>> DSN13.04 - Tekelec

Tekelec: rtrv-secu-dflt; UOUT=30

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Disable inactive accounts

Configure systems to disable accounts that are inactive for more than 30 days, if technically feasible. If the system does not provide this functionality, the ISSO/IAO should review accounts every 30 days to ensure that only needed accounts are active.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.05 V0007960 CAT I Management access points not password protected

8500.2 IA Control: IAIA-2, ECSC-1, IAIA-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1, Chairman Of The Joint Chiefs Of Staff Instruction (CJCSI) 6215.01B; Policy For Department Of Defense Voice Networks C-A-1, Para 2

Vulnerability Management access points (i.e. administrative/maintenance ports, system access, etc.) are not password protected.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Require passwords on all acc

Ensure that all access points are password protected.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.06 V0007961 CAT III Passwords do not meet complexity requirements.

8500.2 IA Control: ECSC-1, IAIA-1, IAIA-2

References: Chairman Of The Joint Chiefs Of Staff Instruction (CJCSI) 6215.01B; Policy For Department Of Defense Voice Networks C-A-1, Para 4, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1

Vulnerability Passwords do not meet complexity requirements.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

>> DSN13.06 - Nortel

>Table OFCENG; MIN_PASSWORD_LENGTH = 8

>> DSN13.06 - Siemens

- DISPPSWDAT; MINIMUM LENGTH FOR PASSWORDS=8

>> DSN13.06 - Tekelec

- rtrv-secu-dflt; MINLEN=8, NUM=1, PUNC=1

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Enforce complex passwords

Enforce a password policy to ensure complex passwords. Configure the system to require passwords to be eight non-repeating characters in length, contain numbers, upper and lower case characters, and a special character, if technically feasible.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.07 V0007962 CAT II Max password age does not meet minimum requirement

8500.2 IA Control: ECSC-1, IAIA-1, IAIA-2

References: Chairman Of The Joint Chiefs Of Staff Instruction (CJCSI) 6215.01B; Policy For Department Of Defense Voice Networks C-A-2, Para 7, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1

Vulnerability Maximum password age does not meet minimum requirements.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

> Review current configuration files of effected devices to confirm compliance.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

>> DSN13.07 - Nortel

>Table OFCENG; PASSWORD_LIFETIME =<90 or ....=<180>> DSN13.07 - Siemens (Manual) - DISPPSWDAT; TIME INTERVAL (DAYS) FOR PASSWORD CHANGE = <90 or ....= <90

>> DSN13.07 - Tekelec

- rtrv-secu-dflt; PAGE=<90 or ....=<180

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Enforce max password age

Ensure password life is no greater than 90 (180) days from the last password change.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.08 V0007963 CAT II Password change interval (24 hours) not enforced

8500.2 IA Control: ECSC-1, IAIA-1, IAIA-2

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1

Vulnerability Users are permitted to change their passwords at an interval of less than 24 hours without ISSO/IAO intervention.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Enforce pswd change interval

Eensure that user passwords are not allowed to be changed for at least 24 hours after change operation.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.09 V0007964 CAT III Password reuse is not set to 8 or greater.

8500.2 IA Control: IAIA-1, ECSC-1, IAIA-2

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1, Chairman Of The Joint Chiefs Of Staff Instruction (CJCSI) 6215.01B; Policy For Department Of Defense Voice Networks C-A-4, Para 10

Vulnerability Password reuse is not set to 8 or greater.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices.

> Review current configuration

> Review current configuration files of effected devices to confirm compliance.

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Enforce password history

Ensure password uniqueness is set to remember 8 passwords.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.10 V0007966 CAT II Passwords can be retrieved / viewed in clear text

8500.2 IA Control: IAIA-2, IAIA-1, ECSC-1

References: Defense Switched Network (DSN) STIG V1R1 Sect. 8.2

Vulnerability User passwords can be retrieved and viewed in clear text by another user.

Checks

>> DSN13.11 - Nortel

>TABLE OFCOPT; PASSWORD_ENCRYPTED =Y

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Ensure encrypted pswd storag

Ensure that the DSN component is provisioned to store all passwords in an encrypted format.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.11 V0007967 CAT II Passwords are displayed in the clear at logon

8500.2 IA Control: IAIA-1, IAIA-2, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1

Vulnerability User passwords are displayed in the clear when logging into the system.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

> Review current configuration files of effected devices to confirm compliance.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Preclude clear text display

Ensure systems are configured not to display passwords in the clear during logon. If hardware or firmware restrict the implementation of this function, upgrade as soon as possible.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.12 V0007968 CAT IV Random password generation not used

8500.2 IA Control: ECSC-1, IAIA-2, IAIA-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1

Vulnerability The option to use passwords that are randomly generated by the DSN component is available but not being used.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

> Review current configuration files of effected devices to confirm compliance.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Randomly generate passwords

Configure the system to randomly generate user passwords if the system provides this functionality.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.13 V0007969 CAT II Access not disabled after password expiration

8500.2 IA Control: IAIA-2, ECSC-1, IAIA-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1

Vulnerability The system is not configured to disable a users account after three notifications of password expiration.

Checks

>> DSN13.14 - Nortel

>TABLE OFCENG; EXPIRED_PASSWORD_GRACE = 3

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices.

> Review current configuration

> Review current configuration files of effected devices to confirm compliance.

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Enforce access disablement

Ensure the DSN component is configured to disable a user account after the user has received three notifications of password expiration.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.14 V0007965 CAT II High level passwords not recorded and controlled

8500.2 IA Control: IAIA-2, IAIA-1, ECSC-1

References: Defense Switched Network (DSN) STIG V1R1 Sect. 8.2

Vulnerability The ISSO/IAO has not recorded the passwords of high level users (ADMIN) used on DSN components and stored them in a secure or controlled manner.

Checks

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> DSN13.14 - Record high level

Record the passwords of high level users and store in a controlled manner.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.15 V0007970 CAT II Crash-restart vulnerabilities are present.

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1

Vulnerability Crash-restart vulnerabilities are present on the DSN system component.

Checks

>> DSN13.15 - Nortel

ensure ENHANCED_PASSWORD_CONTROL is active to prevent system logons after restart on Nortel switches

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

>> DSN13.15 -Verify crash-res

Ensure procedures are in place to verify all system settings after any crash-restart to ensure the system has not reverted to default configuration settings.

>> DSN13.15 - Nortel

Ensure ENHANCED_PASSWORD_CONTROL is active to prevent system logons after restart on Nortel switches

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.16 V0008560 CAT II Management access NOT remotely authenticated

8500.2 IA Control: ECSC-1, IAAC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1

Vulnerability Access to all management system workstations and administrative / management ports is NOT remotely authenticated

Checks

> Review current configuration

> Review current configuration files of effected devices to confirm compliance.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN13.17 V0008559 CAT II Two-factor authentication NOT used

8500.2 IA Control: ECSC-1, IAAC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.1

Vulnerability Strong two-factor authentication is NOT used to access all management system workstations and administrative / management ports on all devices or systems

Checks

> Review current configuration

Review current configuration files of effected devices to confirm compliance

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN14.01 V0007971 CAT II DSN device not installed in a secure location

8500.2 IA Control: ECSC-1, PECF-2

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.8

Vulnerability The DSN system component is not installed in a controlled space with visitor access controls applied.

Checks

> Perform a walk through

Perform a walk through of the facility and confirm compliance via inspection of the effected devices or items

Fixes

> Apply physical security

> Take measures to apply or install or upgrade physical security for system core assets (Switches, Servers,) and transmission devices (network switches, routers, muxes, devices). Limit, control, and document the distribution of keys to access the equipmen

> Apply visitor access control

> Take measures to ensure that all access, and especially visitor access, to key core systems is controlled and documented so that an audit trail can be established if necessary

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN14.02 V0007972 CAT II No SOP for responding to a device compromise

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.8

Vulnerability Documented procedures do not exist that will prepare for a suspected compromise of a DSN component.

Checks

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN15.01 V0007973 CAT II Audit records NOT stored in an unalterable file

8500.2 IA Control: ECSC-1, ECTP-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.3, Chairman Of The Joint Chiefs Of Staff Instruction (CJCSI) 6215.01B; Policy For Department Of Defense Voice Networks Section D-A-A-1

Vulnerability Audit records are NOT stored in an unalterable file and can be accessed by individuals not authorized to analyze switch access activity.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Ensure unalterable audit fil

Ensure that all auditing records are recorded to a device that will not allow any individual to make alterations to their content. Ensure that only authorized individuals have access to these files.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN15.02 V0007974 CAT II Audit records do not record individual identity

8500.2 IA Control: ECAR-2, ECSC-1, ECAR-3, ECAR-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.3, Chairman Of The Joint Chiefs Of Staff Instruction (CJCSI) 6215.01B; Policy For Department Of Defense Voice Networks

Vulnerability Audit records do not record the identity of each person and terminal device having access to switch software or databases.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

>> DSN15.02 - Nortel

Lines similar to the following should be seen in the audit log where SECU101 is a user account SECU101, 102, ********

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

Audit Identity and Terminal

Ensure audit records contain the user and terminal identity.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN15.03 V0007975 CAT II Audit records do not record the time of the access

8500.2 IA Control: ECAR-3, ECSC-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran D-A-A-1, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.3

Vulnerability Audit records do not record the time of the access.

Checks

>> DSN15.03 - Nortel

review TABLXXX for compliance

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

> Review current configuration files of effected devices to confirm compliance.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Ensure auditing records time

Ensure a time stamp is provided by the system on all audit records.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN15.04 V0007976 CAT II Auditing does not record security bypass

8500.2 IA Control: ECLC-1, ECSC-1, ECAR-3

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran D-A-A-1, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.3

Vulnerability The auditing records do not record activities that may change, bypass, or negate safeguards built into the software.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Review current configuration

Review current configuration files of effected devices to confirm compliance

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Audit security bypass

Ensure that the system records commands, actions, and activities executed during each user session that might change, bypass, or negate safeguards built into the software.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN15.05 V0007977 CAT II Audit records not properly archived and stored

8500.2 IA Control: ECRR-1, ECTP-1, ECTB-1, ECSC-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran A-A-8, Para 5-b.10, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.3

Vulnerability Audit record archive and storage do not meet minimum requirements.

Checks

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

> Inspect/Review Documents

Inspect or review the required “documents on file” that are necessary for compliance with the requirement.

> Review audit records

Review audit records that have been stored on-line and off-line.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Retain audit logs for 12 mon

Ensure audit records are stored online for 90 days and offline for 12 months.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN15.06 V0007978 CAT II Audit records are not being reviewed weekly

8500.2 IA Control: ECAT-1, ECRG-1, ECSC-1, ECAT-2

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran A-A-5, Para 3-14, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.3

Vulnerability Audit records are not being reviewed by the ISSO/IAO weekly.

Checks

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Review audit logs weekly

The ISSO/IAO or security auditor should review audit records weekly for suspicious activity.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN15.07 V0008546 CAT II Auditing does NOT record security events

8500.2 IA Control: ECAR-2, ECAR-1, ECAR-3, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.1.3

Vulnerability The auditing process DOES NOT record security relevant actions such as the changing of security levels or categories of information

Checks

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

> Inspect/Review Documents

Inspect or review the required “documents on file” that are necessary for compliance with the requirement.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Audit Security Events

Ensure auditing records security events (Manual) – ensure that the system records security related events and information as follows:

Security relevant actions:
- Logons and logouts

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN16.01 V0007979 CAT II An IAO has not been appointed in writing.

8500.2 IA Control: DCSD-1, PECF-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran A-A-5, Para 3-18, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.1

Vulnerability An Information Systems Security Officer/Information Assurance Officer (ISSO/IAO) is not designated for each telecommunications switching system or DSN Site.

Checks

Inspect or Review Documents

Or review the required “documents on file” that are necessary for compliance with the requirement.

Fixes

Designate an IAO in writing

Establish a DSN ISSO/IAO position. In general, this individual will be responsible for establishing, implementing, monitoring, and controlling the sites telephone system security program which will ensure the evaluation of all components of the sites tel

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN16.02 V0007980 CAT II Site personnel not properly security trained

8500.2 IA Control: ECSC-1, PRTN-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.9, Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran A-A-6, Para 4-5

Vulnerability Site personnel have not received the proper security training and/or are not familiar with the documents located in the security library.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Fixes

Train personnel in security

The ISSO/IAO will establish a security practices plan, as outlined in the DSN Security Guide, to ensure that personnel are familiar with the security practices outlined by applicable documents found in the site’s library and have received the appropriate

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN16.03 V0007981 CAT III Security Certification letters are not on file

8500.2 IA Control: ECAN-1, PECF-2

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.9

Vulnerability The ISSO/IAO does not maintain a DSN Personnel Security Certification letter on file for each person involved in DSN A/NM duties.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Fixes

Document security certificatio

Establish a DSN security awareness-training program. Review all DSN personnel security-related responsibilities and document certification by signing a Personnel Security Certification letter.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN16.04 V0007982 CAT II SAs are not appropriately cleared

8500.2 IA Control: PECF-2, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.9, Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran A-A-6, Para 4.5

Vulnerability System administrators are NOT appropriately cleared.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Inspect or Review Documents

Or review the required “documents on file” that are necessary for compliance with the requirement.

Fixes

Obtain DD Form 2875- all users

Obtain a System Authorization Access Request (SAAR) DD Form 2875 for each DRSN user to validate their need-to-know

Confirm SA clearance

The ISSO/IAO will confirm system administrators are appropriately cleared prior to granting access to DSN systems.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN17.01 V0007983 CAT II Identity of maintenance personnel not recorded

8500.2 IA Control: PECF-1, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.10

Vulnerability Site staff does not verify and record the identity of individuals installing or modifying a device or software.

Checks

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Fixes

Obtain DD Form 2875- all users

Obtain a System Authorization Access Request (SAAR) DD Form 2875 for each DRSN user to validate their need-to-know

Maintain a log of maintainers

The Switch Administrator or ISSO/IAO should maintain a log of personnel who perform maintenance on a DSN component. This list should contain military and civilian personnel including vendor representatives.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN17.02 V0007984 CAT II System images are not being backed up weekly

8500.2 IA Control: ECSC-1, CODB-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran c-12, Para 3-h.2, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.10

Vulnerability System images are not being backed up on a weekly basis to the local system and a copy is not being stored on a removable storage device and/or is not being stored off site.

Checks

> Review current configuration

Review current configuration files of effected devices to confirm compliance

Interview the IAO and/or SA

Interview the IAO and/or SA to determine the source of IPT / VoIP system / device patches. Review patching records.

Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable

DSN17.02 - Nortel

Review table IMGSCHED to ensure that image dumps are regularly scheduled

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

Comply with Policy - Backup

f technically feasible, configure the system to automatically perform weekly backups and record them locally on the component and on removable media. Alternately insure that weekly backups are performed manually. The SA must also ensure the removable medi

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN17.03 V0007985 CAT II SA does not ensure back-up media is available

8500.2 IA Control: ECSC-1, CODB-3, CODB-2, COBR-1, CODB-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.10, Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran C-12, Para 3-h.2

Vulnerability Site staff does not ensure backup media is available and up to date prior to software modification.

Checks

> Interview the IAO or SA

Interview the IAO or SA and confirm compliance through discussion, review of site policy, diagrams, documentation, DAA approvals, etc as applicable.

Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable

Fixes

Comply with Policy - Backup

f technically feasible, configure the system to automatically perform weekly backups and record them locally on the component and on removable media. Alternately insure that weekly backups are performed manually. The SA must also ensure the removable medi

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN17.04 V0008531 CAT II Current software or patches NOT used for security

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.10

Vulnerability The latest software loads and patches are NOT applied to all systems to take advantage of security enhancements.

Checks

> Review current configuration

> Review current configuration files of effected devices to confirm compliance.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN17.05 V0008532 CAT II Maintenance and security patches NOT DAA approved

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.10

Vulnerability Maintenance and security patches are NOT approved by the local DAA prior to installation in the system

Checks

> Review current configuration

Review current configuration files of effected devices to confirm compliance

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN17.06 V0008535 CAT II Major software releases NOT DSN APL listed

8500.2 IA Control: ECSC-1, EBCR-1, DCAS-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.1.10

Vulnerability Major software version upgrades have NOT been tested, certified, and placed on the DSN APL before installation.

Checks

> Review current configuration

Review current configuration files of effected devices to confirm compliance

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

Comply with Policy - DSN APL

Ensure non-certified VoIP systems are not connected to the DSN. Sponsor the system for DSN APL testing and certification.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.01 V0007986 CAT II Modems are not physically protected

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.2, Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran C-20, Para 7-b.5

Vulnerability Modems are not physically protected to prevent unauthorized device changes.

Checks

> Inspect effected devices

Inspect a sampling of effected devices and confirm compliance

> Perform a walk through

Perform a walk through of the facility and confirm compliance via inspection of the effected devices or items

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Ensure modems are secured

Ensure all modems are secured that are used to access the DSN administration/maintenance user ports. Allow only authorized personnel to have physical access to these modems.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.02 V0007987 CAT II A detailed listing of all modems is not maintained

8500.2 IA Control: ECSC-1, DCID-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.2

Vulnerability A detailed listing of all modems is not being maintained.

Checks

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

> Validate modem inventory

Inspect and validate the modem inventory while looking for modems that are installed but have not been approved and inventoried.

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Validate modem inventory

Periodically validate the modem inventory while looking for modems that are installed but have not been approved and inventoried.

> Maintain a modem Inventory

Collect information on all approved modems, including model number, serial number, installed location, etc. Maintain this list / inventory and update as needed.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.03 V0007988 CAT II Unauthorized modems are installed.

8500.2 IA Control: EBCR-1, DCID-1, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.2

Vulnerability Unauthorized modems are installed.

Checks

> Perform a walk through

Perform a walk through of the facility and confirm compliance via inspection of the effected devices or items

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

> Validate modem inventory

Inspect and validate the modem inventory while looking for modems that are installed but have not been approved and inventoried.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Remove unauthorized modems

Remove all modems that are not provided by the Government. The ISSO/IAO may conduct periodic inspections for unauthorized modems.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.04 V0007989 CAT II Modem phone lines are not restricted

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.2, Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran C-20, Para7-b.5

Vulnerability Modem phone lines are not restricted and configured to their mission required purpose (i.e. inward/outward dial only).

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Restrict modem lines

Ensure that all modem lines are restricted to single line operation and configured to their mission required purpose (inward or outward dial only), without any special features (i.e. call forwarding). DSN System Administrators will ensure that the modems

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.05 V0007990 CAT II Modem phone lines are not restricted - single-line

8500.2 IA Control: ECSC-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran C-20, Para 7-b.4, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.2

Vulnerability Modem phone lines are not restricted to single-line operation.

Checks

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

> Inspect effected devices

Inspect a sampling of effected devices and confirm compliance

Fixes

> Use single-line phone lines

Ensure that only single-line phone lines are used for modem access.

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.06 V0007991 CAT IV ANI is available but not being used

8500.2 IA Control: ECSC-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran C-20, Para 7-b.6, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.2

Vulnerability The option of Automatic Number Identification (ANI) is available but not being used.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

Fixes

> Use ANI if available

> Ensure the use of the the ANI feature, if available, for all modems connected to DSN system administration/maintenance dial-up ports. Maintain and review ANI logs periodically. Audit records should be stored for a period of twelve months.

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.07 V0007992 CAT II Authentication is not required for every session

8500.2 IA Control: ECSC-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran C-A-2, Para 5, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.1

Vulnerability Authentication is not required for every session requested.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Require auth. for each sessi

Ensure that all interfaces to the DSN component require authentication before a session is granted.

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.08 V0007993 CAT III The "callback" feature is not being used.

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.2, Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran C-F-1, C-F-2

Vulnerability The option to use the "callback" feature for remote access is not being used.

Checks

> Review current configuration

Review current configuration files of effected devices to confirm compliance

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

> Inspect effected devices

Inspect a sampling of effected devices and confirm compliance

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Use callback if available

> The ISSO/IAO should ensure that all DSN components are using the callback feature, if this feature is available.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.09 V0007994 CAT IV FIPS Link encryption mechanisms are not being used

8500.2 IA Control: ECCT-1, ECSC-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "Defense-in-Depth: Information Assuran C-26, Para 2-d, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.1

Vulnerability FIPS 140-2 validated Link encryption mechanisms are not being used to provide end-to-end security of all data streams entering the remote access port of a telephone switch.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Use FIPS Val. Link Encryptio

Ensure that FIPS 140-2 validated link encryption mechanisms are implemented for all dial-up/remote connections to the administration/maintenance ports of the DSN system.

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.10 V0007995 CAT IV 2-factor authentication not used for remote acce

8500.2 IA Control: ECSC-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran C-26, Para 3-a, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.1

Vulnerability The option to use two-factor authentication when accessing remote access ports is not being used.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices.

> Interview the IAO/SA - Gen

Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable.

Fixes

> Use 2-factor auth. for remot

Ensure policies and configurations are in place for remote access ports to require two-factor authentication.

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.11 V0007996 CAT II Admin./ maintenance ports are not being controlled

8500.2 IA Control: ECSC-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran C-F-1, C-F-2

Vulnerability Administrative/maintenance ports are not being controlled by deactivating or physically disconnecting remote access devices when not in use.

Checks

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

>> DSN18.11 - Nortel

> LOGINCONTROL ALL QUERY. (SET TO DISABLE ON LOGOUT)

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Disconnect remote access

Ensure that all remote access devices are deactivated or disconnected when not in use.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.12 V0007997 CAT II Idle connections DO NOT disconnect in 15 min.

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.1

Vulnerability Idle connections DO NOT disconnect in 15 min.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices.

>> DSN18.12 -NORTEL

>LOGINCONTROL ALL QUERY. (MAX IDLE TIME =15 MIN).

Fixes

> Ensure sessions time out

The system administrator will ensure that the timeout for unattended user administration/maintenance ports is set for no longer than 15 minutes, if technically feasible.

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.13 V0007998 CAT II Maint ports do not lock out after 3 failed attempt

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.1, Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran C-A-3, Para 9-a

Vulnerability The DSN component is not configured to be unavailable for 60 seconds after 3 consecutive failed logon attempts.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

>> DSN18.13 - Nortel

>LOGINCONTROL ALL QUERY. (MAX LOGIN RETRIES = 3; SET TO DISABLE ON LOGIN FAIL)

>> DSN18.13 - Siemens

DISP SECTHR; NO. OF FALSE USERID INPUTS=3; NO. OF FALSE PASSWORD INPUTS = 3; LOCK TIME CAUSED BY FALSE PASSWORD INPUT= 1 minute

Fixes

> Enable failed login lockout

Ensure the system is configured to make the port unavailable for 60 seconds after 3 failed logon attempts.

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.14 V0007999 CAT II Serial Mgmt. Ports do not drop interrupted session

8500.2 IA Control: ECSC-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran C-F-2, Para 5, Sec e, DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.2

Vulnerability Serial management/maintenance ports are not configured to “force out” or drop any interrupted user session.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices. Inspect configuration files as applicable.

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

>> DSN18.14 - Nortel

> LOGINCONTROL ALL QUERY. (SET TO DISABLE ON OPEN COND)

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

> Ensure session ends on inter

> Configure the DSN component to force out users when the session is interrupted.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.15 V0008518 CAT II An OOB Management network NOT STIG compliant

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.3

Vulnerability An OOB Management DOES NOT comply with the Enclave and/or Network Infrastructure STIGs.

Checks

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.16 V0008517 CAT II OOB management network are NOT dedicated

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.

Vulnerability OOB management network are NOT dedicated to management of like or associated systems

Checks

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN18.17 V0008516 CAT II Network Mgmt. Ports do not drop interrupted sessio

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.3.3

Vulnerability Network management/maintenance ports are not configured to “force out” or drop any user session that is interrupted for more than 15 seconds.

Checks

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices.

Fixes

> Comply with Policy - General

Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN19.01 V0008000 CAT II Login banner is non-existent or not DOD approved.

8500.2 IA Control: ECWM-1, ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 3.3.4, Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran C-C-1

Vulnerability Login banner is non-existent or does not meet DOD requirements.

Checks

> Demonstrate Compliance

Have the IAO or SA demonstrate compliance with the requirement; minimally on a sampling of the related or effected devices.

Fixes

Configure logon banners

The Switch Administrator should configure the DSN component to display the approved DOD login banner.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN20.01 V0008515 CAT I A SMU is NOT installed in a secure location

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 5

Vulnerability A SMU component is not installed in a controlled space with visitor access controls applied.

Checks

> Inspect Physical Security

> Perform a walk through of the facility to confirm that all DSN core and transmission devices that are part of the system are located in a secure room or locked cabinet.

Fixes

> Apply physical security

> Take measures to apply or install or upgrade physical security for system core assets (Switches, Servers,) and transmission devices (network switches, routers, muxes, devices). Limit, control, and document the distribution of keys to access the equipmen

> Apply visitor access control

> Take measures to ensure that all access, and especially visitor access, to key core systems is controlled and documented so that an audit trail can be established if necessary

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN20.02 V0008514 CAT III SMU ADIMSS connection is NOT dedicated

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 5

Vulnerability The SMU ADIMSS connection is NOT dedicated to the ADIMSS network

Checks

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN20.03 V0008513 CAT II ADIMSS/SMU server NOT dedicated to ADIMSS

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 5

Vulnerability The ADIMSS server connected to the SMU is NOT dedicated to ADIMSS functions.

Checks

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

DSN20.04 V0008512 CAT II SMU Mgmt. port connected to NON-mgmt. network

8500.2 IA Control: ECSC-1

References: DOD Telecommunications and Defense Switched Network (DSN) STIG Section 5

Vulnerability The SMU management port or management workstations is improperly connected to a network that is not dedicated to management of the SMU.

Checks

> Interview IAO/ SA - Gen

> Interview the IAO and/or SA to confirm compliance through discussion, review of site policy and procedures, diagrams, documentation, configuration files, logs, records, DAA/other approvals, etc as applicable

Fixes

> Comply with Policy - General

> Implement processes / procedures, generate documents, and/or adjust configuration(s) / architecture, as necessary to comply with policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes: